

to those individuals and their families impacted by muscular dystrophy that Congress—yes, we are—is committed to finding a cure. We will find the resources to do this. This legislation is yet another step, and I urge my colleagues to vote “yes.”

Mr. BURGESS. Mr. Speaker, let me close by saying this is a good bill, and I urge all Members to support it.

I yield back the balance of my time.

Mr. WAXMAN. Mr. Speaker, I want to express my support for H.R. 594, the Paul D. Wellstone Muscular Dystrophy Community Assistance, Research and Education (MD CARE) Amendments of 2014.

The Centers for Disease Control and Prevention and the National Institutes of Health oversee a number of research, surveillance, and educational efforts involving muscular dystrophy.

H.R. 594 will build upon the federal government's current activities regarding muscular dystrophy. Scientific advances have extended the lives of individuals living with forms of muscular dystrophy—like Duchenne. Today's legislation will help better incorporate the needs of adults with muscular dystrophy into current work in this area.

Congressman ENGEL and Congressman BURGESS should be recognized for their leadership on this issue. I would also like to thank Chairman UPTON, Chairman PITTS, Ranking Member PALLONE, and all of our staff for their work in advancing this bill through the Energy and Commerce Committee.

I support H.R. 594 and urge my colleagues to do the same.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. BURGESS) that the House suspend the rules and pass the bill, H.R. 594, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

The title of the bill was amended so as to read: “A bill to amend the Public Health Service Act relating to Federal research on muscular dystrophy, and other purposes.”

A motion to reconsider was laid on the table.

SAFE AND SECURE FEDERAL WEBSITES ACT OF 2014

Mr. BENTIVOLIO. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3635) to ensure the functionality and security of new Federal websites that collect personally identifiable information, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3635

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Safe and Secure Federal Websites Act of 2014”.

SEC. 2. ENSURING FUNCTIONALITY AND SECURITY OF NEW FEDERAL WEBSITES THAT COLLECT PERSONALLY IDENTIFIABLE INFORMATION.

(a) CERTIFICATION REQUIREMENT.—

(1) *IN GENERAL.*—Except as otherwise provided under this subsection, an agency may not deploy or make available to the public a new Federal PII website until the date on which the chief information officer of the agency submits a certification to Congress that the website is fully functional and secure.

(2) *TRANSITION.*—In the case of a new Federal PII website that is operational on the date of the enactment of this Act, paragraph (1) shall not apply until the end of the 90-day period beginning on such date of enactment. If the certification required under paragraph (1) for such website has not been submitted to Congress before the end of such period, the head of the responsible agency shall render the website inaccessible to the public until such certification is submitted to Congress.

(3) *EXCEPTION FOR BETA WEBSITE WITH EXPLICIT PERMISSION.*—Paragraph (1) shall not apply to a website (or portion thereof) that is in a development or testing phase, if the following conditions are met:

(A) A member of the public may access PII-related portions of the website only after executing an agreement that acknowledges the risks involved.

(B) No agency compelled, enjoined, or otherwise provided incentives for such a member to access the website for such purposes.

(4) *CONSTRUCTION.*—Nothing in this section shall be construed as applying to a website that is operated entirely by an entity (such as a State or locality) that is independent of the Federal Government, regardless of the receipt of funding in support of such website from the Federal Government.

(b) *DEFINITIONS.*—In this section:

(1) *AGENCY.*—The term “agency” has the meaning given that term under section 551 of title 5, United States Code.

(2) *FULLY FUNCTIONAL.*—The term “fully functional” means, with respect to a new Federal PII website, that the website can fully support the activities for which it is designed or intended with regard to the eliciting, collection, storage, or maintenance of personally identifiable information, including handling a volume of queries relating to such information commensurate with the purpose for which the website is designed.

(3) *NEW FEDERAL PERSONALLY IDENTIFIABLE INFORMATION WEBSITE (NEW FEDERAL PII WEBSITE).*—The terms “new Federal personally identifiable information website” and “new Federal PII website” mean a website that—

(A) is operated by (or under a contract with) an agency;

(B) elicits, collects, stores, or maintains personally identifiable information of individuals and is accessible to the public; and

(C) is first made accessible to the public and collects or stores personally identifiable information of individuals, on or after October 1, 2012.

(4) *OPERATIONAL.*—The term “operational” means, with respect to a website, that such website elicits, collects, stores, or maintains personally identifiable information of members of the public and is accessible to the public.

(5) *PERSONALLY IDENTIFIABLE INFORMATION (PII).*—The terms “personally identifiable information” and “PII” mean any information about an individual elicited, collected, stored, or maintained by an agency, including—

(A) any information that can be used to distinguish or trace the identity of an individual, such as a name, a social security number, a date and place of birth, a mother's maiden name, or biometric records; and

(B) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

(6) *RESPONSIBLE AGENCY.*—The term “responsible agency” means, with respect to a new Federal PII website, the agency that is responsible for the operation (whether directly or through contracts with other entities) of the website.

(7) *SECURE.*—The term “secure” means, with respect to a new Federal PII website, that the following requirements are met:

(A) The website is in compliance with subchapter III of chapter 35 of title 44, United States Code.

(B) The website ensures that personally identifiable information elicited, collected, stored, or maintained in connection with the website is captured at the latest possible step in a user input sequence.

(C) The responsible agency for the website has taken reasonable efforts to minimize domain name confusion, including through additional domain registrations.

(D) The responsible agency requires all personnel who have access to personally identifiable information in connection with the website to have completed a Standard Form 85P and signed a non-disclosure agreement with respect to personally identifiable information, and the agency takes proper precautions to ensure only trustworthy persons may access such information.

(E) The responsible agency maintains (either directly or through contract) sufficient personnel to respond in a timely manner to issues relating to the proper functioning and security of the website, and to monitor on an ongoing basis existing and emerging security threats to the website.

(8) *STATE.*—The term “State” means each State of the United States, the District of Columbia, each territory or possession of the United States, and each federally recognized Indian tribe.

SEC. 3. PRIVACY BREACH REQUIREMENTS.

(a) *INFORMATION SECURITY AMENDMENT.*—Subchapter III of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

“§3550. Privacy breach requirements

“(a) *POLICIES AND PROCEDURES.*—The Director of the Office of Management and Budget shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

“(1) not later than 72 hours after the agency discovers such a breach, or discovers evidence that reasonably indicates such a breach has occurred, notice to the individuals whose personally identifiable information could be compromised as a result of such breach;

“(2) timely reporting to a Federal cybersecurity center, as designated by the Director of the Office of Management and Budget; and

“(3) any additional actions that the Director finds necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services.

“(b) *REQUIRED AGENCY ACTION.*—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or control of the agency comply with policies and procedures established by the Director of the Office of Management and Budget under subsection (a).

“(c) *REPORT.*—Not later than March 1 of each year, the Director of the Office of Management and Budget shall report to Congress on agency compliance with the policies and procedures established under subsection (a).

“(d) *FEDERAL CYBERSECURITY CENTER DESIGNATED.*—The term ‘Federal cybersecurity center’ means any of the following:

“(1) The Department of Defense Cyber Crime Center.

“(2) The Intelligence Community Incident Response Center.

“(3) The United States Cyber Command Joint Operations Center.

“(4) The National Cyber Investigative Joint Task Force.

“(5) Central Security Service Threat Operations Center of the National Security Agency.

“(6) The United States Computer Emergency Readiness Team.

“(7) Any successor to a center, team, or task force described in paragraphs (1) through (6).

“(8) Any center that the Director of the Office of Management and Budget determines is appropriate to carry out the requirements of this section.”.

(b) **TECHNICAL AND CONFORMING AMENDMENT.**—The table of sections for subchapter III of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

“3550. Privacy breach requirements.”.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Michigan (Mr. BENTIVOLIO) and the gentleman from Massachusetts (Mr. LYNCH) each will control 20 minutes.

The Chair recognizes the gentleman from Michigan.

GENERAL LEAVE

Mr. BENTIVOLIO. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Michigan?

There was no objection.

Mr. BENTIVOLIO. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, we, as Members of Congress, have been sent here to protect the people's right to privacy, not take it away. My bill, H.R. 3635, will help to instill confidence in Americans that their privacy and personal information is secure. H.R. 3635 will help ensure the functionality and security of Federal Web sites. The escalation of security breaches involving personally identifiable information has contributed to the loss of millions of records over the past few years, both within and outside the Federal Government.

Web sites that fail to meet their intended function are a waste of taxpayer dollars and can result in needless frustration to the end user who is trying to access a Federal service or benefit. The harm to the Federal Government is the loss of public trust, as well as potential legal liability or remediation costs that the taxpayer may ultimately bear.

H.R. 3635 guards against the loss of the public's trust by requiring agency chief information officers certify that Federal Web sites collecting personally identifiable information are fully functional and secure. In addition, the bill requires agencies to notify affected individuals that their personally identifiable information may have been compromised within 72 hours of a known or suspected data breach.

I would like to thank Chairman ISSA, Ranking Member CUMMINGS, and Congressman CONNOLLY for their support of the bill, along with Chairman MCCAUL and committee staff.

I reserve the balance of my time.

Mr. LYNCH. Mr. Speaker, I yield myself such time as I may consume.

I think we all agree that Federal agency Web sites must be secure in

order to protect taxpayers from being the victims of an information security breach. For that reason, I support the measure before us, the Safe and Secure Federal Websites Act. The recent data breaches at Target, Neiman Marcus, and other retail establishments affected more than 100 million Americans. The importance of information security cannot be overstated.

It is the responsibility of Congress to ensure that the Federal Government is not the source of these types of data breaches and to ensure that the personally identifiable information of American citizens is not compromised through Federal Web sites. This bill would require agency chief information officers to certify to Congress the functionality and security of new or substantially modified Web sites that contain personally identifiable information. It would also require that existing Web sites that contain personally identifiable information meet these security requirements within 90 days.

We are not known for our speed around here, so I am not entirely sure that that will be enough for agencies to secure existing Web sites. I hope, as this bill moves forward in the legislation, the timeliness issue is addressed. However, overall, these requirements are positive, beginning steps in preventing harmful data breaches within the Federal Government.

I also want to take special time to mention and to thank Congressman CONNOLLY from Virginia for his positive contribution to this legislation and for his work on data security issues. Mr. CONNOLLY's amendment to this legislation closes the loopholes in Federal privacy requirements and streamlines Federal oversight of agency implementation of privacy policies and procedures pertaining to agency responses to security incidents involving personally identifiable information.

I join with the gentleman from Virginia in sincerely hoping that we can continue to work together to move this bill forward in a bipartisan manner. I also hope that we can work together to ensure that this bill is compatible with the existing framework of the Federal Security Management Act.

I have no further speakers, and I yield back the balance of my time.

Mr. BENTIVOLIO. Mr. Speaker, I yield myself such time as I may consume.

This bill has 126 cosponsors and passed out of committee with bipartisan support. I strongly urge passage of this bill to protect the privacy of Americans accessing Federal Web sites and support this bipartisan legislation.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Michigan (Mr. BENTIVOLIO) that the House suspend the rules and pass the bill, H.R. 3635, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

LANCE CORPORAL WESLEY G. DAVIDS AND CAPTAIN NICHOLAS J. ROZANSKI MEMORIAL POST OFFICE

Mr. BENTIVOLIO. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4919) to designate the facility of the United States Postal Service located at 715 Shawan Falls Drive in Dublin, Ohio, as the “Lance Corporal Wesley G. Davids and Captain Nicholas J. Rozanski Memorial Post Office”.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4919

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. LANCE CORPORAL WESLEY G. DAVIDS AND CAPTAIN NICHOLAS J. ROZANSKI MEMORIAL POST OFFICE.

(a) **DESIGNATION.**—The facility of the United States Postal Service located at 715 Shawan Falls Drive in Dublin, Ohio, shall be known and designated as the “Lance Corporal Wesley G. Davids and Captain Nicholas J. Rozanski Memorial Post Office”.

(b) **REFERENCES.**—Any reference in a law, map, regulation, document, paper, or other record of the United States to the facility referred to in subsection (a) shall be deemed to be a reference to the “Lance Corporal Wesley G. Davids and Captain Nicholas J. Rozanski Memorial Post Office”.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Michigan (Mr. BENTIVOLIO) and the gentleman from Massachusetts (Mr. LYNCH) each will control 20 minutes.

The Chair recognizes the gentleman from Michigan.

GENERAL LEAVE

Mr. BENTIVOLIO. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous remarks on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Michigan?

There was no objection.

Mr. BENTIVOLIO. Mr. Speaker, I yield such time as he may consume to the gentleman from Ohio (Mr. TIBERI).

Mr. TIBERI. Mr. Speaker, I thank the gentleman from Michigan as well as the chairman of the Oversight and Government Reform Committee, Chairman ISSA, for their ability to pass this through committee and bring it to the floor today.

Mr. Speaker, I rise in support of my bill, H.R. 4919, to designate the United States Postal Service facility located at 715 Shawan Falls Drive in Dublin, Ohio, as the Lance Corporal Wesley G. Davids and Captain Nicholas J. Rozanski Memorial Post Office.

Marine Lance Corporal Wesley Davids was 16 years old and still attending Dublin Scioto High School when he